# ESX Firewall Switching Agent Guide

FORE SYSTEMS®

FORE SYSTEMS®

MANU 0378-01

U.S. Government Restricted Rights. If you are licensing the Software on behalf of the U.S. Government (“Government”), the following provisions apply to you. If the Software is supplied to the Department of Defense (“DoD”), it is classified as “Commercial Computer Software” under paragraph 252.227-7014 of the DoD Supplement to the Federal Acquisition Regulations (“DFARS”) (or any successor regulations) and the Government is acquiring only the license rights granted herein (the license rights customarily provided to non-Government users). If the Software is supplied to any unit or agency of the Government other than DoD, it is classified as “Restricted Computer Software” and the Government’s rights in the Software are defined in paragraph 52.227-19 of the Federal Acquisition Regulations (“FAR”) (or any successor regulations) or, in the cases of NASA, in paragraph 18.52.227-86 of the NASA Supplement to the FAR (or any successor regulations).

ESX is a trademark of FORE Systems, Inc.

NT is a registered trademark of Microsoft Corporation.

FireWall-1 is a registered trademark of Check Point$^{TM}$ Software Technologies Inc.

In the U.S.A., you can contact FORE Systems’ Technical Support using any one of the following methods:

- You can receive online support via TACtics Online at: http://www.fore.com
- You can contact Technical Support via e-mail at: support@fore.com
- You can telephone your questions to Technical Support at: 1-800-671-FORE (3673) or +1 724-742-6999
- You can FAX your questions to Technical Support at:+1 724-742-7900

Technical support for non-U.S.A. customers should be handled through your local distributor.

No matter which method is used for support, please be prepared to provide your support contract ID number, the serial number(s) of the product(s), and as much information as possible describing your problem/question.

IMPORTANT

CAREFULLY READ THE FOLLOWING TERMS, CONDITIONS AND RESTRICTIONS BEFORE INSTALLATION AND USE OF ANY SOFTWARE PROGRAMS PROVIDED BY FORE SYSTEMS, INCORPORATED. OPENING THE SEALED SOFTWARE PACKAGE AND/OR INSTALLATION OR USE OF SUCH SOFTWARE PROGRAMS SHALL BE DEEMED ACCEPTANCE OF THESE TERMS, CONDITIONS AND RESTRICTIONS.

IF YOU DO NOT AGREE WITH AND ACCEPT THESE TERMS, CONDITIONS AND RESTRICTIONS, PROMPTLY RETURN ALL SUCH SOFTWARE AND HARDWARE PRODUCTS TO FORE SYSTEMS, INC. AND ANY FEES PAID FOR SUCH PRODUCTS WILL BE REFUNDED.

1. LICENSE

Subject to the terms and restrictions set forth in this License, FORE Systems, Inc. (“FORE”) grants a non-exclusive non-transferable (except as provided herein) license to use the software programs (“Programs”) for use with FORE and/or third party hardware products.

2. COPYRIGHT

The Programs, and all related documentation, are protected by copyright and title to all programs is retained by FORE. You may not copy or otherwise use the Programs, in whole or part, except as expressly permitted in this License. You must reproduce and maintain the copyright notice on any authorized copy you make or use of the Programs.

3. RESTRICTIONS ON USE AND TRANSFER

The Programs may be copied solely for installation and back-up purposes. You may not modify the Programs in any manner without the prior written approval of FORE. You may physically transfer the Programs and this License, along with the related FORE hardware, if applicable, to another party only if (i) the other party accepts the terms, conditions and restrictions of this License, (ii) all copies of Programs and related documentation that are not transferred to the other party are destroyed or returned to FORE, (iii) the related FORE hardware for programs designed solely to operate on FORE hardware, is also transferred to the other party, and (iv) you comply with all applicable laws including any import/export control regulations.

4. LIMITED WARRANTY

FORE warrants that the Programs will perform substantially in accordance with the accompanying documentation for a period of ninety (90) days from the date of shipment. This warranty is void if failure is the result of accident, abuse or misuse.

FORE warrants that any media on which the Programs are recorded will be free from defects in materials and workmanship under normal use for a period of ninety (90) days from the date the Programs are delivered to you. If a defect in any such media should occur during this 90-day period, the media may be returned to FORE, at 1000 FORE Drive, Warrendale, Pennsylvania 15086-7502 U.S.A., and FORE will replace the media without charge to you. FORE shall have no responsibility to replace media if the failure of media results from accident, abuse, or misuse.

The program contains third party software which is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the program could lead directly to death, personal injury, or severe physical or environmental damage (“High Risk Activities”). Accordingly, FORE and FORE's third party licensors specifically disclaim any express or implied warranty of fitness for High Risk Activities.

EXCEPT FOR THE WARRANTIES SPECIFICALLY STATED IN THIS ARTICLE, FORE HEREBY DISCLAIMS ALL EXPRESS OR IMPLIED WARRANTIES OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you. This limited warranty gives you specific legal rights, and you may also have other rights which vary from jurisdiction to jurisdiction.

5. LIMITATION OF LIABILITY

Your exclusive remedy and the entire liability of FORE related to the Programs shall be, at FORE's option: (i) refund of the price paid for the Programs, (ii) correction of the Programs so they perform as warranted, or in the case of media failure, replacement of media as provided above. In no event will FORE or anyone else who has been involved in the creation, production, or delivery of the Programs be liable for any damages, including, without limitation, direct, incidental or consequential damages, loss of anticipated profits or benefits, resulting from the use of the Programs, even if FORE has been advised of the possibility of such damages.

6. TERM

This License is effective until terminated. You may terminate this License at any time by destroying all copies of the Programs and related documentation. This License will terminate automatically if you fail to comply with any term or condition of this License, including any attempt to transfer a copy of the Programs to another party except as provided in this License. You agree that, upon such termination, you will destroy all copies of the Programs and related documentation.

7. CONFIDENTIALITY

You agree that the source code applicable to the Programs is confidential and proprietary to FORE. Accordingly, you may not decompile, reverse engineer or otherwise manipulate the Programs so as to derive such source code.

8. U.S. GOVERNMENT RESTRICTED RIGHTS LEGEND

If you are licensing the Software on behalf of the U.S. Government (“Government”), the following provisions apply. If the Software is supplied to the Department of Defense (“DoD”), it is classified as “Commercial Computer Software” under paragraph 252.227-7014 of the DoD Supplement to the Federal Acquisition Regulations (“DFARS”) (or any successor regulations) and the Government is acquiring only the license rights granted herein (the license rights customarily provided to non- Government users). If the Software is supplied to any unit or agency of the Government other than DoD, it is classified as “Restricted Computer Software” and the Government's rights in the Software are defined in paragraph 52.227-19 of the Federal Acquisition Regulations (“FAR”) (or any successor regulations) or, in the case of NASA, in paragraph 18.52.227-86 of the NASA Supplement to the FAR (or any successor regulations). Use, duplication or disclosure by the Government is subject to the restrictions set forth in such sections. The Contractor for the Programs is FORE Systems, Inc., 1000 FORE Drive, Warrendale, Pennsylvania 15086-7502.

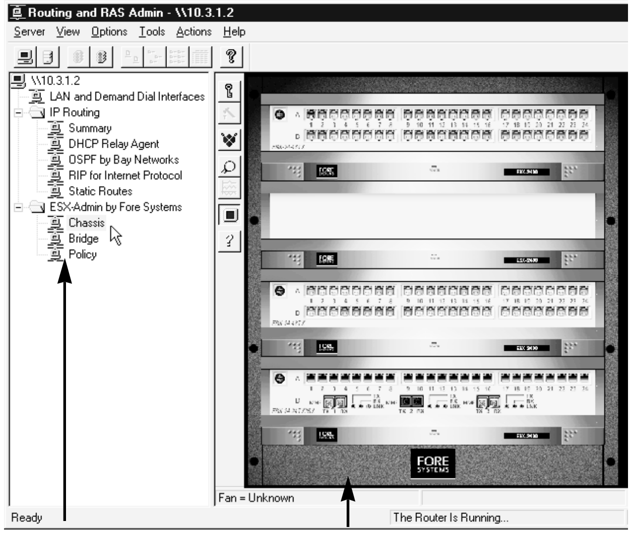
YOUR USE OF THE PROGRAMS ACKNOWLEDGES THAT YOU HAVE READ THIS END-USER SOFTWARE LICENSE, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS, CONDITIONS AND RESTRICTIONS. YOU FURTHER AGREE THAT THIS LICENSE IS THE COMPLETE AND EXCLUSIVE STATEMENT OF YOUR AGREEMENT WITH FORE AND SUPERSEDES ANY PROPOSAL OR PRIOR AGREEMENT, ORAL OR WRITTEN, AND ANY OTHER COMMUNICATIONS RELATING TO THE SUBJECT MATTER OF THIS LICENSE.

## Navigating Using the ESX-Admin Interface

The Firewall Switching Agent Guide provides flowcharts that describe navigation paths. These paths help you access configuration menus and wizards. It also gives procedural steps and examples to show how to configure the system.

| **Flowchart Shape** | **Represents** |
|---|---|
| In Tree View | ***Starting point for navigation****–often tree view or display view, and occasionally navigation begins with a main configuration page.* |
| Right Click Chassis Icon<br>Select Configure Chassis | ***A navigation step****:*<br>• *Right click–displays a pull down menu*<br>• *Select–selects an icon or menu item using one of the following techniques:*<br>  • *Left mouse click–picks a single item*<br>  • *Drag click–activates a selection window*<br>  • *Shift click–selects contiguous icons*<br>  • *Control shift click–selects non-contiguous icons* |
| Modify Chassis Configuration Page | ***A procedure or task*** |

## Example: Tree View and Chassis Display



***Tree View***
*Select configuration menus and view status*

***Display View***
*Enter editing mode, select ports, and view system status.*

In the example above, clicking the *chassis icon*, shown in the *tree view*, fills the *display view* with a graphic view of the chassis. Navigation starts by positioning the mouse in either the tree view or in the display view.

**To select multiple consecutive ports:**
When configuring ports on the switch you may want to select multiple ports and configure them identically, To select multiple, consecutive ports, press the CTRL key while you hold down the left mouse button activating a lasso, and use the lasso to select multiple consecutive ports.

### Accessing Context-sensitive and Topic Online Help

- To access ***context sensitive online help***, first click on the ? icon on the ***horizontal menu bar*** at the top of the screen. When a ? appears next to the mouse pointer, click on an area in a dialog box to display a help message for a field, a control button or area within the dialog box.
- To access ***ESX-Admin help topics***, click on the ? icon on the ***vertical menu bar*** at the top of the screen. An index of help topics will appear on the screen

### Using Icons to Access ESX-Admin Commands

The *vertical menu bar* contains seven icons, stacked vertically in the border area between the tree view and the display view. By clicking an icon you can access commands directly from the main menu.. A description of menu bar icons and their associated commands follows:

**Edit Mode -** ***toggle edit mode & display edit menu***

**Configure -** ***set switch/port parameters***

**Edit Policy -** ***configure policies on the switch***

**Show Port Info -** ***display port statistics***

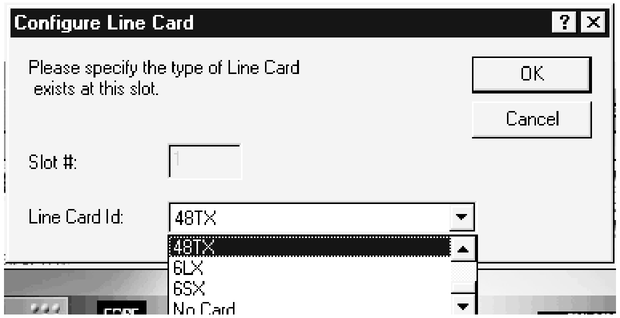
**ESX-Mon -** ***access the monitoring facility***

**Scale Window -** ***expand or shrink the display***

**Online Help -** ***view ESX-Admin help topics***

### Example: Vertical and Horizontal Menu Bars

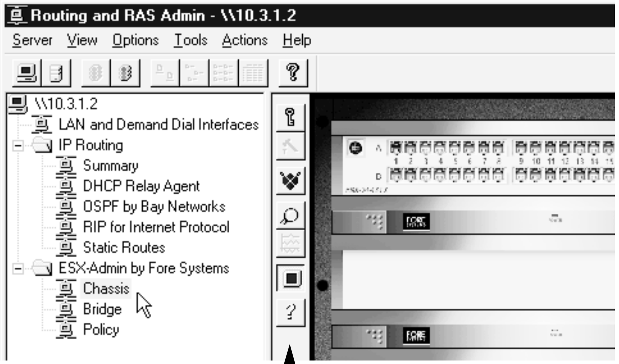
***Horizontal Menu Bar ? Icon****- Context-sensitive Online Help*


Configure Line Card

Please specify the type of Line Card exists at this slot.

Slot #: 1

Line Card Id: 48TX


Routing and RAS Admin - \\10.3.1.2

***Vertical Menu Bar Icons -*** *Short cut to commands*

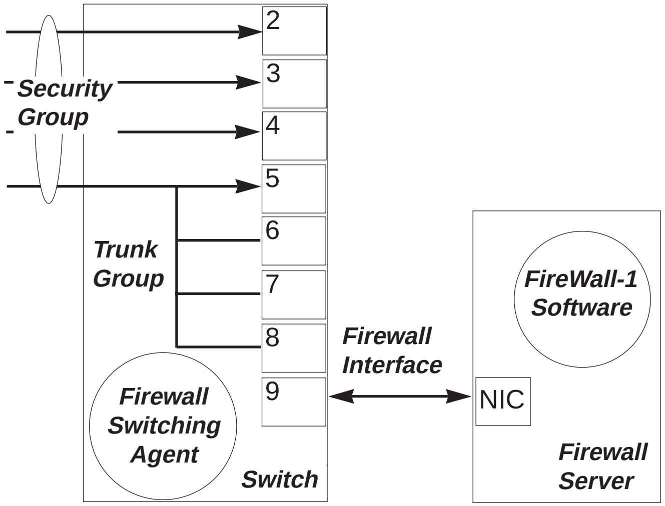
The Firewall Switching Agent Guide provides an overview of firewalls, describes requirements for configuring a firewall server, and provides detailed procedures that will help you set up a firewall on your network.

The Firewall Switching Agent Guide contains the following sections:

## 1–Firewall Overview

A FORE Systems firewall is made up of these components shown in the example below and described in the following text:

- Firewall Switching Agent
- Firewall interface
- Firewall server
- FireWall-1TM software
- Security group
- Switch
- Trunk Group



**Example: Firewall Component Overview**

**Firewall Switching Agent**–A combination of ASICs, ASIC microcode, and management software which, together, implement the Fast Path forwarding functions of CheckPoint's FireWall-1TM software.

**Note:** FireWall-1TM is a Registered Trademark.

**Firewall interface**–a bidirectional connection you establish between a port on the *switch* (*Port 9 in the example)* and a NIC on the *firewall server*.

- The *Firewall Switching* Agent forwards each packet that requires further inspection than Fast Path can provide across the *firewall interface* to the *FireWall-1 software*
- The *FireWall-1TM software* validates the packet against its rule/policy database, and if the packet passes inspection, the *firewall server* returns the packet to the switch

**Firewall server**–an NT or Unix device running *FireWall-1 software.*

**FireWall-1 software**–Check Point's *FireWall-1* receives frames requiring closer inspection from the *Firewall Switching Agent*, performs firewall checks and sends frames back.

**Security group**–a group of ports on the switch that shares a pool of firewall servers. A *security group* can include trunk groups along with individual ports. You can include all ports on the switch in a single security group or establish up to 16 security groups on a single switch.
In the example, switch ports 2 - 4 and the *trunk group* (ports 5 - 8) are members of the *security group.*

**Note:** The *Firewall Switching Agent* checks each frame that is received on an input port of a security group. This implementation may differ from other firewall security implementations.

**Switch**–A FORE Systems ESX-2400 or ESX-4800 Switch.

**Trunk Group** –Two or more ports seen by the switch as a single, logical port. A trunk group can join a *security group*.

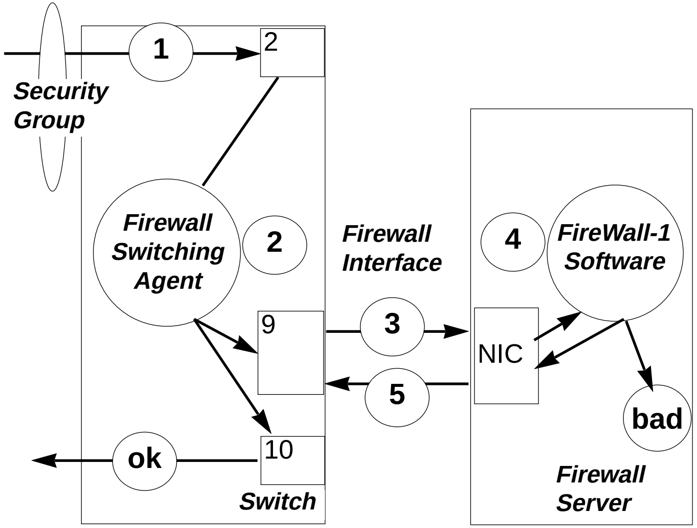
## Firewall Packet Flow

The following example shows the packet flow through the firewall, describing the sequence of events that occur when a frame is received by port 2, a member of a security group, destined for an interface attached to port 10.

As in the previous example:

- Port 9 on the switch provides the firewall interface along with the NIC in the firewall server
- The Firewall Switching Agent running in the switch and the FireWall-1™ software running on the firewall server perform validation checking

**The Sequence of Events:**



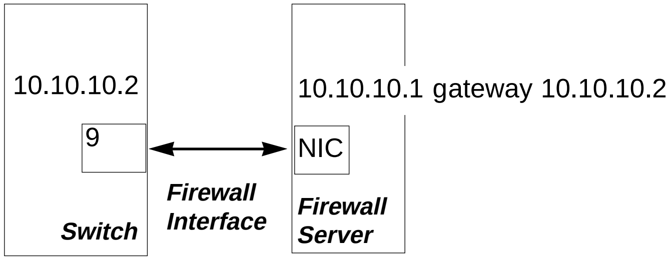
**Example: Firewall Packet Flow**

1. Port 2 receives a packet destined for an interface attached to port 10.
2. The Firewall Switching Agent inspects the packet:
   - If OK the packet is forwarded out on port 10
   - If the packet requires further inspection, step 3 occurs
3. The packet is sent across the firewall interface to the firewall server via port 9.
4. The FireWall-1™ software validates the packet:
   - If not OK the packet is dropped
   - If OK, step 5 occurs
5. The packet is sent across the firewall interface to the switch via the NIC and forwarded by the switch on port 10, the packet’s intended destination

## 2–Setting up a Firewall Server

Before you configure the Firewall Switching Agent, set up the Firewall Server by completing the following tasks:

**1.** Connect an Ethernet cable between a network adapter in the firewall server and a port on the switch.
**Note**: This cable forms the firewall connection between the switch and the firewall server. To establish a secure interface, attach the switch and the firewall server, directly, rather than via a hub.
**Caution**: The port to which you connect the cable on the switch can not be assigned to a security group.



**Example: Setting Up Switch and Firewall Server IP Addresses**

**2.** Set up the IP addresses on the switch and the firewall server that are required to establish the firewall interface between the switch and the firewall server. See the example and following text for details.
**Note**: The IP addresses for the switch and the firewall server that form the firewall interface must be on the same subnet.

- On the switch, assign an IP Address to the firewall interface port on the switch.
  *In the example, Port 9's IP address = 10.10.10.2*
  *See Chapter 7 of the* ***ESX Switch Administrator's Guide*** *for details on assigning IP addresses to ports.*
- On the firewall server: assign an IP Address to the firewall server's NIC, and assign a default gateway pointing to the IP address of the switch's firewall interface port.
  *In the example, the NIC's IP address = 10.10.10.1 and the NIC's default gateway = 10.10.10.2*
  **Note**: Define the IP addresses for the switch and the firewall server that form the firewall interface before you create a security group.

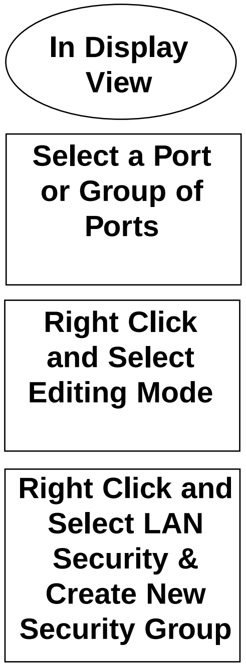
**3.** After you set up the IP addresses on the switch and the firewall server, assign IP addresses to the members of the security group that you will create in the next section.

# 3–Creating a Security Group

You can create a security group by following this three-part procedure:

- Select a port or group of ports
- Access the LAN Security Configuration page
- Configure a LAN Security Server

**Note:** You can include all the ports on the switch, including trunk groups in a security group, and you can define up to 16 security groups on a single switch.



**In Display View**

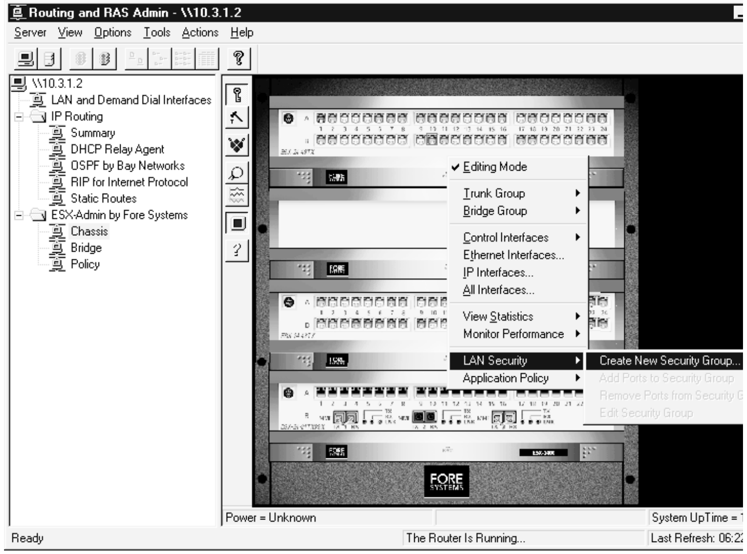
**Select a Port or Group of Ports**

**Right Click and Select Editing Mode**

**Right Click and Select LAN Security & Create New Security Group**

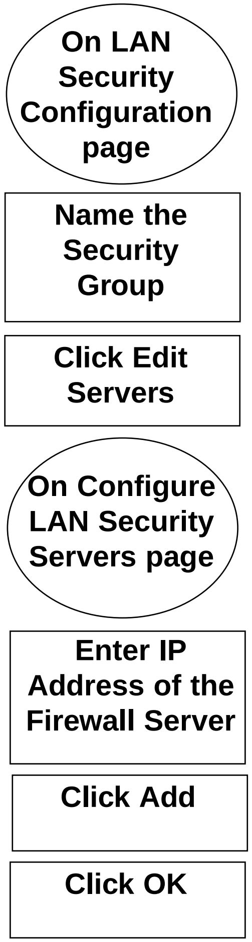
In the Display View:

1. Select a port or group of ports.
2. Right Click in Display View and select Editing Mode.
3. Right Click again in Display View and select LAN Security and Create New Security Group to display the LAN Security Configuration page.



# 3–Creating a Security Group (Continued)

Continue the process of creating a security group using the LAN Security Configuration page.



**On LAN Security Configuration page**

**Name the Security Group**

**Click Edit Servers**

**On Configure LAN Security Servers page**

**Enter IP Address of the Firewall Server**

**Click Add**

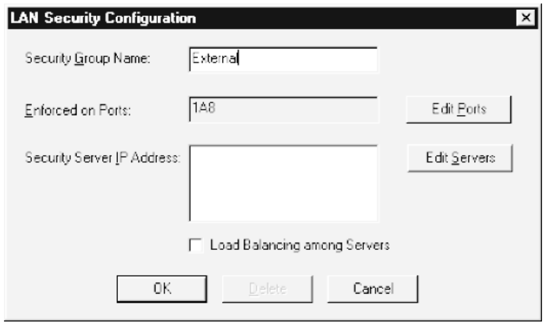
**Click OK**

On LAN Security Configuration page:

1. Name the Security Group.
2. Click Edit Servers to display the Configure LAN Security Servers page.

On Configure LAN Security Servers page:

3. Enter the IP address of the firewall server.
   In the example *10.10.10.1*
   **Note:** You can add multiple IP addresses if you have multiple firewall servers in a redundant configuration.
4. Click Add to update the Server Addresses field on the Configure LAN Security Servers page.
   **Note**: The IP address of the server you added will appear in the Servers Available: window.



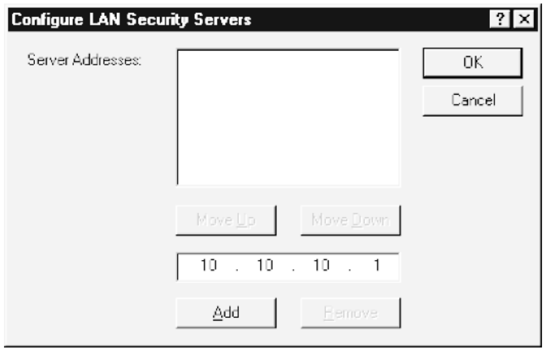
LAN Security Configuration

Security Group Name: External

Enforced on Ports: 1A8

Security Server IP Address:

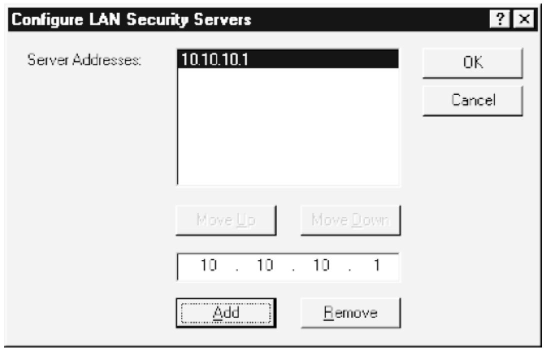
☐ Load Balancing among Servers



Configure LAN Security Servers

Server Addresses:

10 . 10 . 10 . 1



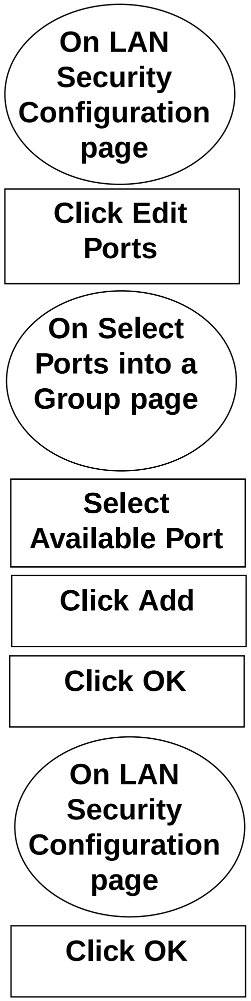
Configure LAN Security Servers

Server Addresses: 10.10.10.1

10 . 10 . 10 . 1

## 3–Creating a Security Group (Continued)

While you create a security group, you can add additional ports by:



**On LAN Security Configuration page**

**Click Edit Ports**

**On Select Ports into a Group page**

**Select Available Port**

**Click Add**

**Click OK**

**On LAN Security Configuration page**

**Click OK**

On LAN Security Configuration page:

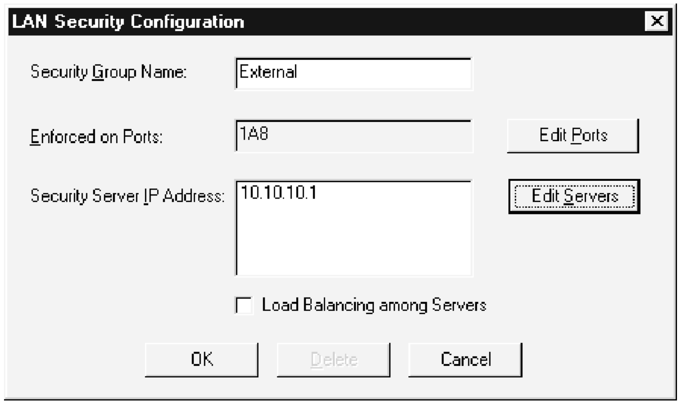
1. Click the Edit Ports button to display the Select Ports into a Group page.

On Select Ports into a Group page:

2. Select a port you want to add from the Available Ports: window.
3. Click Add.
4. Click OK to add the port and return to the LAN Security Configuration Page,

On LAN Security Configuration page:

5. Click OK to establish the new security group.



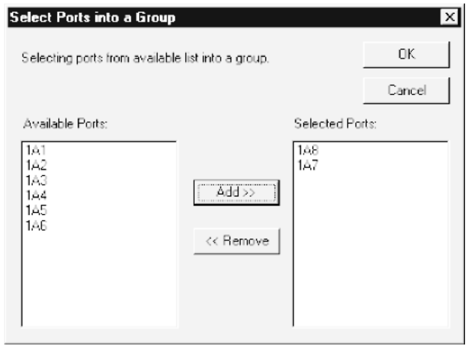
LAN Security Configuration

Security Group Name: External

Enforced on Ports: 1A8

Security Server IP Address: 10.10.10.1

☐ Load Balancing among Servers

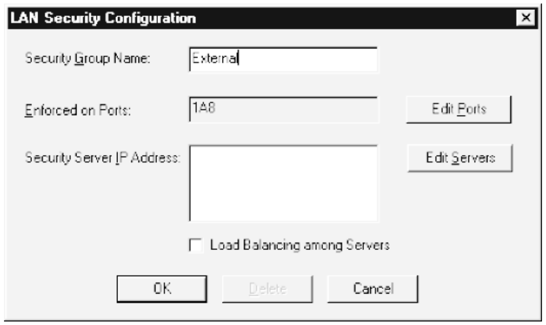


Select Ports into a Group

Selecting ports from available list into a group.

Available Ports: 1A1, 1A2, 1A3, 1A4, 1A5, 1A6

Selected Ports: 1A8, 1A7



LAN Security Configuration

Security Group Name: External

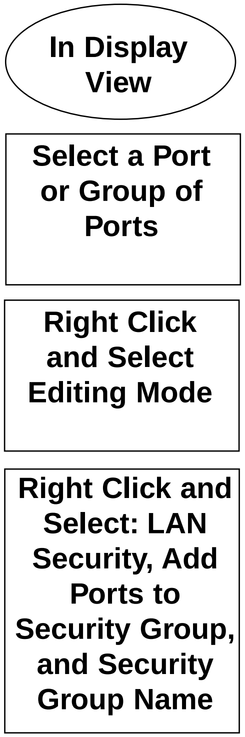
Enforced on Ports: 1A8

Security Server IP Address:

☐ Load Balancing among Servers

## 4–Adding Ports to A Security Group

After you create a security group, you can add additional ports.



In Display View

Select a Port or Group of Ports

Right Click and Select Editing Mode

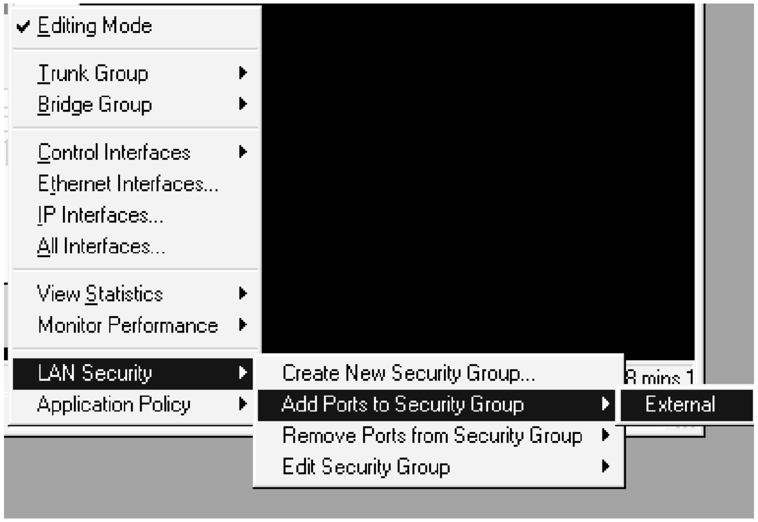
Right Click and Select: LAN Security, Add Ports to Security Group, and Security Group Name

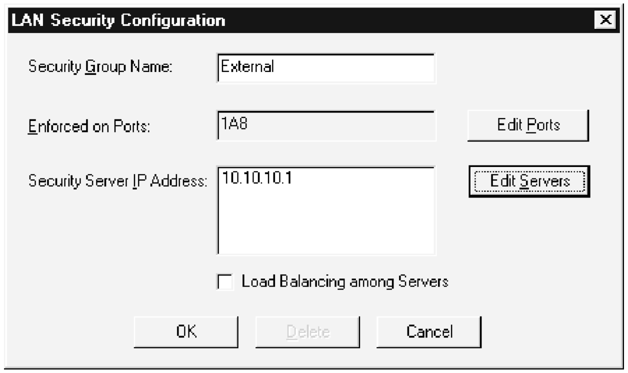
In Display View:

1. Select the port or group of ports you want to add to the security group.
2. Right Click in Display View and select Editing Mode.
3. Right Click again in Display View and select:
   - LAN Security
   - Add Ports to Security Group
   - Name of security group

   to display the LAN Security Configuration page–*the Port ID of the port you added will show up in the Enforced on Ports: window.*

**Note:** You also can add ports from the LAN Security page by clicking Edit Ports and following the instructions on the previous page.





LAN Security Configuration

Security Group Name: External

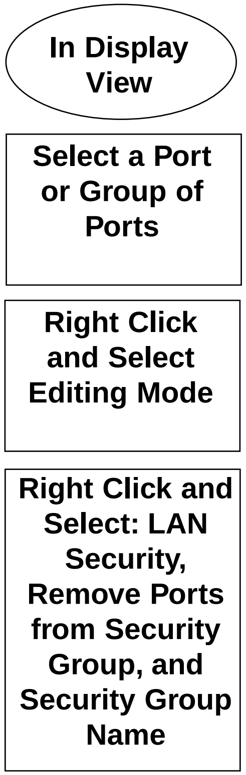
Enforced on Ports: 1A8

Security Server IP Address: 10.10.10.1

□ Load Balancing among Servers

## 5–Removing Ports from a Security Group

Follow this procedure to remove ports from a LAN Security Group:



In Display View

Select a Port or Group of Ports

Right Click and Select Editing Mode

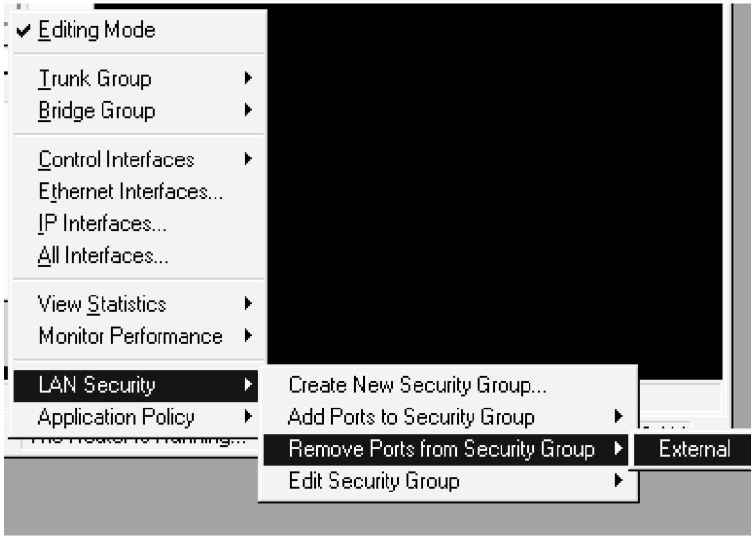
Right Click and Select: LAN Security, Remove Ports from Security Group, and Security Group Name

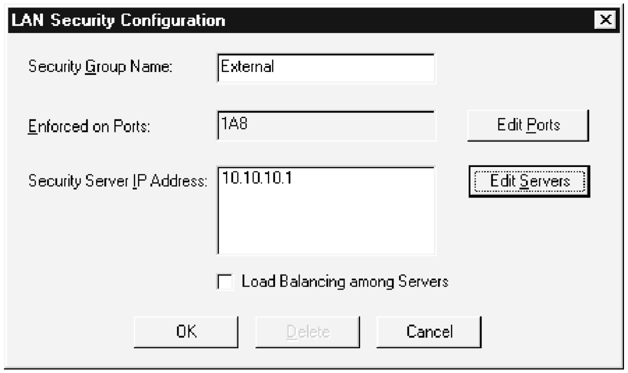
In Display View:

1. Select the port or group of ports you want to remove from the security group.
2. Right Click in Display View and select Editing Mode.
3. Right Click again in Display View and select:
   - LAN Security
   - Remove Ports from Security Group
   - Name of security group

   to display the LAN Security Configuration page–*the Port ID of the port you removed will* *<u>not</u>* *show up in the Enforced on Ports: window.*

**Note:** From the LAN Security page you can remove ports by following the instructions on the next page.





LAN Security Configuration

Security Group Name: External

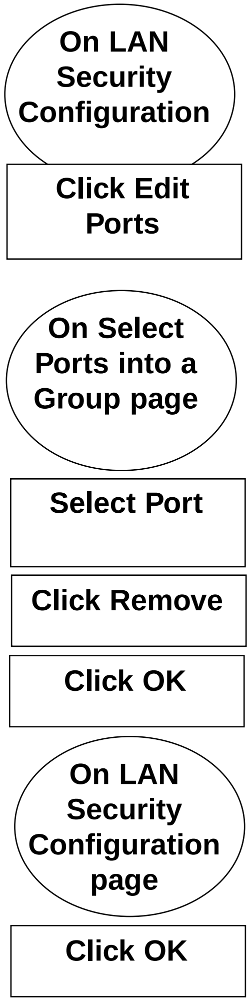
Enforced on Ports: 1A8

Security Server IP Address: 10.10.10.1

☐ Load Balancing among Servers

## 5–Removing Ports (continued)

Continue this procedure to remove ports from a LAN Security Group:



On LAN Security Configuration
Click Edit Ports
On Select Ports into a Group page
Select Port
Click Remove
Click OK
On LAN Security Configuration page
Click OK

On LAN Security Configuration page:

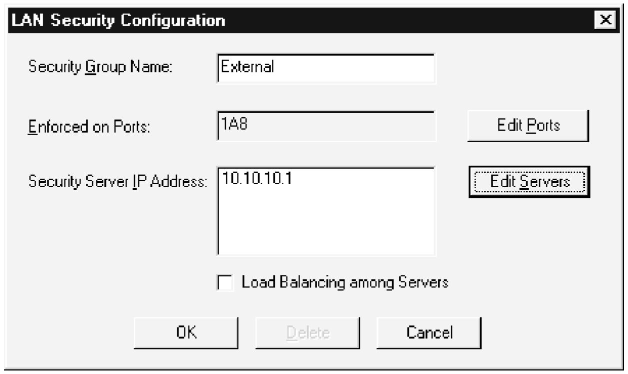
1. Click the Edit Ports button to display the Select Ports into a Group page.

On Select Ports into a Group page:

2. Select a port you want to remove from the Available Ports: window.
3. Click Remove.
4. Click OK to close and return to the LAN Security Configuration Page

On LAN Security Configuration page:

5. Click OK to have the new security group configuration take effect.



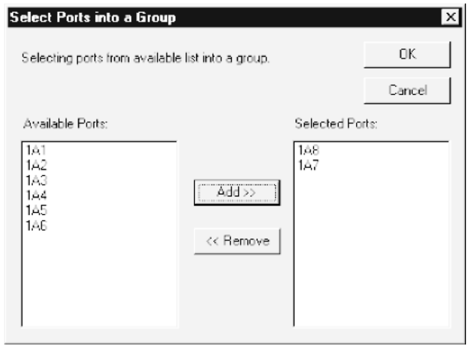
LAN Security Configuration

Security Group Name: External

Enforced on Ports: 1A8

Security Server IP Address: 10.10.10.1

□ Load Balancing among Servers

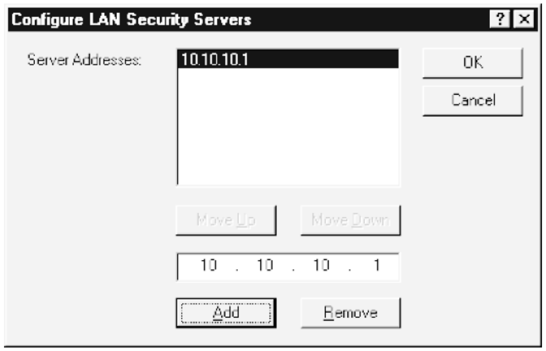


Select Ports into a Group

Selecting ports from available list into a group.

Available Ports: 1A1, 1A2, 1A3, 1A4, 1A5, 1A6

Selected Ports: 1A8, 1A7



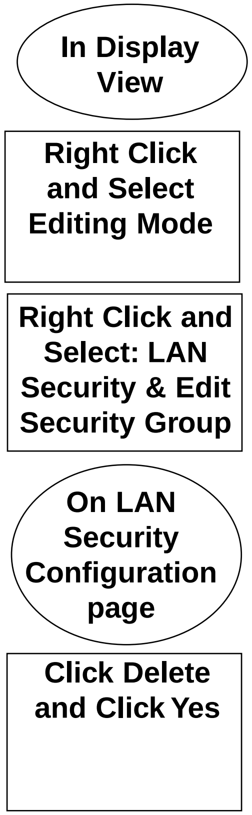
Configure LAN Security Servers

Server Addresses: 10.10.10.1

10 . 10 . 10 . 1

## 6–Deleting a Security Group

After you create a security group,follow this procedure to delete it.



**In Display View**

**Right Click and Select Editing Mode**

**Right Click and Select: LAN Security & Edit Security Group**

**On LAN Security Configuration page**

**Click Delete and Click Yes**

In Display View:

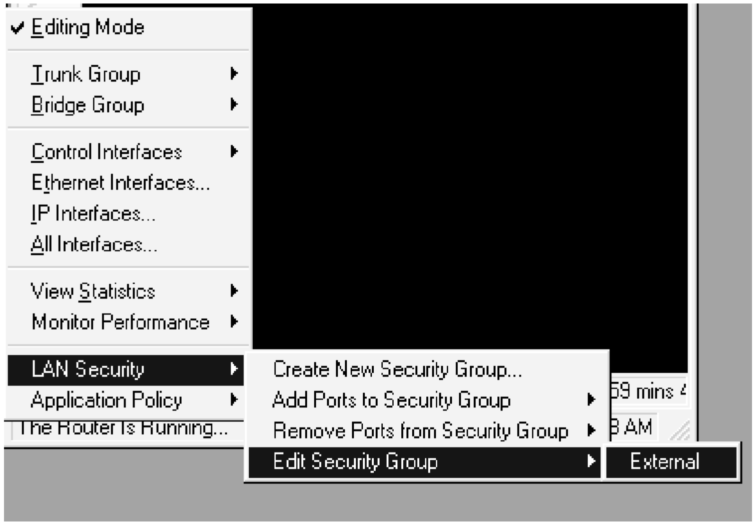
1. Right Click in Display View and select Editing Mode.
2. Right Click again in Display View and select:
   - LAN Security
   - Edit Security Group
   - Name of security group

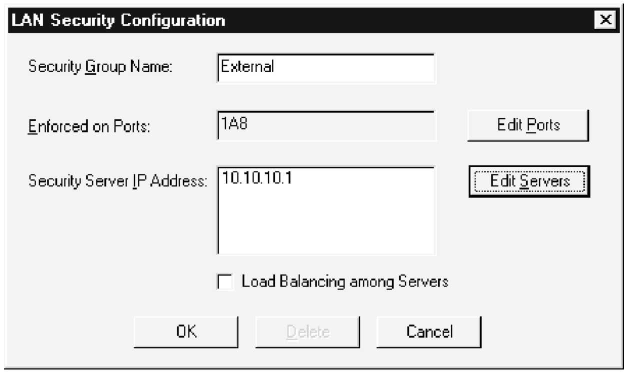
   to display the LAN Security Configuration page

   **Note:** The name of the security group you want to remove will appear in the Security Group Name: window.

On LAN Security Configuration page:

1. Click Delete to display a confirmation window and click Yes.





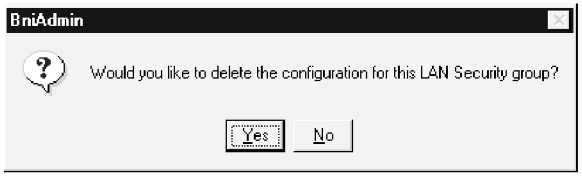
LAN Security Configuration

Security Group Name: External

Enforced on Ports: 1A8

Security Server IP Address: 10.10.10.1

☐ Load Balancing among Servers



BniAdmin

Would you like to delete the configuration for this LAN Security group?